Claims

1. Method for application layer authentication of subscribers connected to the authenticating network domain by a 2G or 2.5G GPRS core network or a 3G UMTS network, characterised by using data which are assembled by the network layer during establishment of a PDP context in GPRS networks.

2. Method according to claim 1, comprising the step that during PDP context establishment the Serving GPRS Support Node (SGSN) is authenticating the subscriber using the A3/A8 algorithm based on the end devices SIM card.

3. Method according to any preceding claim, comprising the step that a Gateway GPRS Support Node (1) receives a context creation request and queries a registration server (2) to get an IP address assigned for the particular PDP context, and within the context the registration server 2 receives the MSISDN and/or the IMSI of the subscriber and stores for each PDP context a pair of IP address and IMSI/MSISDN in a session database (3).

4. Method according to any preceding claim, comprising the step that a proxy server (5) is provided which checks IMSI/MSISDN from a radius server (2) database (3) and IMSI/MSISDN from application domain database (4) for match.

5. Method according to any preceding claim, comprising the step that if the IMSI/MSISDN pairs are matching, the radius server (5) checks the subscribers IP address in

the IP network layer for match with the IP address assigned by the Radius server (3).

6. Method according to any preceding claim, comprising the step that the proxy server (5) parses the application layer for IP addresses given in the headers of registration messages and checks for match with the IP address which was already checked for match with the IP address assigned by the radius server (2).

7. Method according to any preceding claim, comprising the step that in all subsequent messages arriving at the proxy server (5), it checks for match of IP address in the IP packet overhead field for source address with that in the application layer protocol header fields and verifies the matching pairs against the IP address assigned by the Radius server (2).

8. Method according to any preceding claim, that a routing module (7) is provided which is the standard entry point for all messages and decides by evaluation of PrivID which network node will handle the message.

9. System of units in a mobile telecommunication network, characterised that at least a first authentication unit (2) is connected via a data line to a second unit (5; 6) which assembles data according to the method of claim 1.

10. System according to claim 9, wherein the first unit comprises a registration server (2).

11. System according to claim 9 or 10, wherein the first unit (2) is connected to a session database (3).

12. System according to any of claims 9 to 11, wherein the second unit comprises a proxy server (5).

13. System according to any of claims 9 to 12, wherein the second unit comprises a Proxy Call State Control Function (6).

14. System according to any of claims 9 to 13, wherein the second unit (5; 6) is connected to a subscriber database (4).

15. System according to any of claims 9 to 14, wherein a routing module (7) is provided decides by evaluation of PrivID which network node will handle the message.